BW

1409

JP409321789A Dec. 12, 1997 L14: 1 of 3

NETWORK SYSTEM WITH DUPLEXED ROUTERS AND FAULT COUNTERMEASURE METHOD FOR IT

INVENTOR: YAMATANI, SHOGO
HAMADA, TAKUSHI
MIZOKAWA, SADAO
TANJI, MASAYUKI
MARUYAMA, HISAYUKI
INOUE, HIROBUMI
APPLICANT: HITACHI LTD
APPL NO: JP 08136854
DATE FILED: May 30, 1996
INT-CL: H04L12/46; H04L12/28; H04L12/66; H04L29/14

ABSTRACT:

PROBLEM TO BE SOLVED: To improve the availability of a network and to avoid the increase of the load on the CPU of a computer by reducing the time for switching a route from an active router to a stand-by router to be shorter than that at the time of using RIP(routing information protocol) in a network system with duplexed routers.

SOLUTION: One of the duplexed routers is set to be an active router and the other is set to be a stand-by router and they are assigned with respectively the same logic address (IP(internet protocol) address) and different physical addresses (MAC(medium access control) addresses), and the communication controller 11 of a computer (a1) on a network holds this logical address and physical address. Then when the communication controller 11 communicates with another computer (b-1) through routers α and β, the physical address of the active router is used for communication. On the other hand, when an **ARP** (address resolution protocol) response message is not transmitted to the active router α in spite of requesting it from the active router α, the router is switched to the stand-by router β by judging the **fault** to be generated.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報**（Ａ）　(11)特許出願公開番号

特開平9－321789

(43)公開日　平成９年(1997)12月12日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ		技術表示箇所
Ｈ０４Ｌ	12/46			Ｈ０４Ｌ	11/00	３１０Ｃ
	12/28		9466－5K		11/20	Ｂ
	12/66				13/00	３１１
	29/14					

審査請求　未請求　請求項の数10　ＯＬ　（全 32 頁）

(21)出願番号　特願平8－136854

(22)出願日　平成８年(1996)５月30日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　山谷　昇吾
茨城県日立市大みか町五丁目２番１号　株式会社日立製作所大みか工場内

(72)発明者　濱田　卓志
茨城県日立市大みか町五丁目２番１号　株式会社日立製作所大みか工場内

(72)発明者　溝河　貞生
茨城県日立市大みか町五丁目２番１号　株式会社日立製作所大みか工場内

(74)代理人　弁理士　高橋　明夫　（外１名）

最終頁に続く

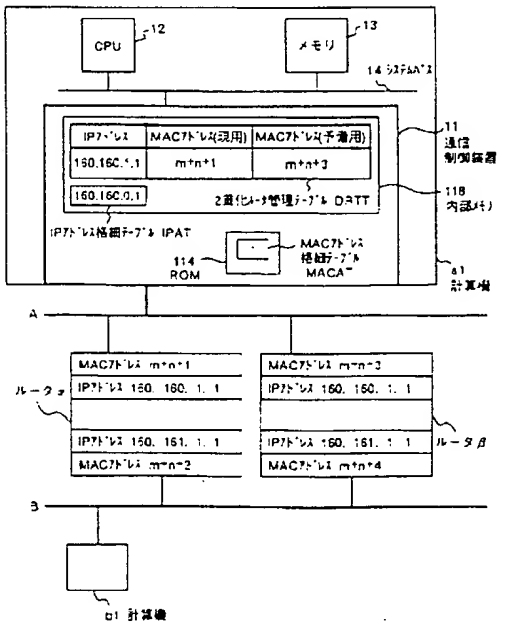
(54)【発明の名称】　ルータが２重化されたネットワークシステムおよびルータが２重化されたネットワークシステムの障害対策方法

(57)【要約】

【課題】ルータが２重化されたネットワークシステムにおいて、現用のルータから予備用のルータに経路を切り替えるときには、その切替時間をＲＩＰ使用時より短縮し、ネットワークの可用性を向上させる，かつ、そのときに、計算機のＣＰＵの負荷を増加させない，

【解決手段】２重化されたルータの一方を現用ルータ、他の一方を予備用ルータとして、各々同一の論理アドレス（ＩＰアドレス）と異なった物理アドレス（ＭＡＣアドレス）とを割り当て、ネットワーク上の計算機の通信制御装置は、この論理アドレスと物理アドレスとを保持する，そして、この通信制御装置が、ルータを介して他の計算機と通信するときには、現用ルータの物理アドレスを用いて通信する．一方、現用ルータから、ＡＲＰレスポンスメッセージを求めて、送信されてこないときには、障害が発生したものとして、予備用ルータに切り替えて通信する，

図　1



1

【特許請求の範囲】

【請求項１】　一つ以上のネットワークをルータを介して接続し、しかも、そのルータが２重化されたネットワークシステムにおいて、

前記ネットワークに接続された計算機は、通信制御装置を有し、

この計算機は、各々有する通信制御装置によって通信し、

また、前記２重化されたルータは、一方を現用ルータ、他の一方を予備用ルータとして、

各々同一の論理アドレスと、異なった物理アドレスとが割り当てられ、

前記通信制御装置は、

前記２重化されたルータの論理アドレスと物理アドレスとを保持する手段を有し、

この通信制御装置が、

ルータを介して他の計算機と通信するときには、前記現用ルータの物理アドレスを用いて通信し、

２重化されたルータに対して、周期的に論理アドレスから物理アドレスを求めるリクエストメッセージを送信し、

その送信したリクエストメッセージの返答となるレスポンスメッセージが、ルータから送信されてくるか否かを、２重化された各々のルータに対して監視し、

ルータからレスポンスメッセージが送信されてこないときには、そのルータに障害が発生したものとして、

もし、前記現用ルータに障害が発生したとされたときには、

ルータを介して他の計算機と通信するときに、前記予備用ルータの物理アドレスを用いて通信するように切り替えることを特徴とするルータが２重化されたネットワークシステム。

【請求項２】　前記通信制御装置が、

前記２重化されたルータに割り当てられる論理アドレスと物理アドレスとを、計算機より受け取って、

それらを２重化されたルータの論理アドレスと物理アドレスとを保持する手段に設定することを特徴とする請求項１記載のルータが２重化されたネットワークシステム。

【請求項３】　前記通信制御装置が、

前記２重化されたルータに割り当てられる論理アドレスと物理アドレスとを、２重化されたルータ各々に対して送信される前記論理アドレスから物理アドレスを求めるリクエストメッセージの返答となるレスポンスメッセージから得て、

それらを２重化されたルータの論理アドレスと物理アドレスとを保持する手段に設定することを特徴とする請求項１記載のルータが２重化されたネットワークシステム。

【請求項４】　前記現用ルータに障害が発生されたときには、

前記予備用ルータを新たな現用ルータとし、

現用ルータを取換えて、新たな予備用ルータとして、

前記通信制御装置が、

２重化されたルータの論理アドレスと物理アドレスとを保持する手段に、

前記新たな現用ルータと前記新たな予備用ルータとに割り当てられる論理アドレスと物理アドレスとを、それぞれ設定することを特徴とする請求項１ないし請求項３記載のいずれかのルータが２重化されたネットワークシステム。

【請求項５】　前記物理アドレスが、ＭＡＣ（Media Access Control）アドレスであり、

前記論理アドレスが、ＩＰ（Internet Protocol）アドレスであり、

前記論理アドレスから、物理アドレスを求めるリクエストメッセージが、ＡＲＰ（Address Resolution Protocol）リクエストメッセージで、その返答となるレスポンスメッセージが、ＡＲＰレスポンスメッセージであることを特徴とする請求項１ないし請求項４記載のいずれかのルータが２重化されたネットワークシステム。

【請求項６】　一つ以上のネットワークをルータを介して接続し、しかも、そのルータが２重化されたネットワークシステムの障害対策方法において、

前記ネットワークに接続された計算機は、通信制御装置を有し、

この計算機は、各々有する通信制御装置によって通信し、

また、前記２重化されたルータは、一方を現用ルータ、他の一方を予備用ルータとして、

各々同一の論理アドレスと、異なった物理アドレスとが割り当てられ、

前記通信制御装置は、

前記２重化されたルータの論理アドレスと物理アドレスとを保持する手段を有し、

この通信制御装置が、

ルータを介して他の計算機と通信するときには、前記現用ルータの物理アドレスを用いて通信し、

２重化されたルータに対して、周期的に論理アドレスから物理アドレスを求めるリクエストメッセージを送信し、

その送信したリクエストメッセージの返答となるレスポンスメッセージが、ルータから送信されてくるか否かを、２重化された各々のルータに対して監視し、

ルータからレスポンスメッセージが送信されてこないときには、そのルータに障害が発生したものとして、

もし、前記現用ルータに障害が発生したとされたときには、

ルータを介して他の計算機と通信するときに、前記予備用ルータの物理アドレスを用いて通信するように切り替

えることを特徴とするルータが2重化されたネットワークシステムの障害対策方法。

【請求項7】　前記通信制御装置が、

前記2重化されたルータに割り当てられる論理アドレスと物理アドレスとを、計算機より受け取って、

それらを2重化されたルータの論理アドレスと物理アドレスとを保持する手段に設定することを特徴とする請求項6記載のルータが2重化されたネットワークシステムの障害対策方法。

【請求項8】　前記通信制御装置が、

前記2重化されたルータに割り当てられる論理アドレスと物理アドレスとを、2重化されたルータ各々に対して送信される前記論理アドレスから物理アドレスを求めるリクエストメッセージの返答となるレスポンスメッセージから得て、

それらを2重化されたルータの論理アドレスと物理アドレスとを保持する手段に設定することを特徴とする請求項6記載のルータが2重化されたネットワークシステムの障害対策方法。

【請求項9】　前記現用ルータに障害が発生されたときには、

前記予備用ルータを新たな現用ルータとし、

現用ルータを取換えて、新たな予備用ルータとして、

前記通信制御装置が、

2重化されたルータの論理アドレスと物理アドレスとを保持する手段に、

前記新たな現用ルータと前記新たな予備用ルータとに割り当てられる論理アドレスと物理アドレスとを、それぞれ設定することを特徴とする請求項6ないし請求項8記載のいずれかのルータが2重化されたネットワークシステムの障害対策方法。

【請求項10】　前記物理アドレスが、MAC（Media Access Control）アドレスであり、

前記論理アドレスが、IP（Internet Protocol）アドレスであり、

前記論理アドレスから、物理アドレスを求めるリクエストメッセージが、ARP（Address Resolution Protocol）リクエストメッセージで、その返答となるレスポンスメッセージが、ARPレスポンスメッセージであることを特徴とする請求項6ないし請求項9記載のいずれかのルータが2重化されたネットワークシステムの障害対策方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ルータが2重化されたネットワークシステムおよびルータが2重化されたネットワークシステムの障害対策方法に係り、ルータを2重化して信頼性を高めるシステムであって、しかも、無停止で運用する必要性のあるネットワークシステムに用いて好適なネットワークシステムに関する。

【0002】

【従来の技術】近年、異なるネットワークに接続する計算機間で通信する場合に、ネットワーク間でデータを中継し、経路選択する機器として、ルータを用いるケースが増えてきている。

【0003】一般に、ルータが経路を選択するプロトコル（「ルーティングプロトコル」といわれる）としては、静的な情報としてルーティング情報を保持するスタティックルーティングと、動的に情報を交換して、それに基づいてルーティングをおこなうダイナミックルーティングと言われる二種類の方法がある。

【0004】ところで、このようなルータで2つのネットワークを接続する際に、1台のルータでネットワーク間を接続している場合には、そのルータに障害が発生すると、ネットワーク間での通信ができなくなる。

【0005】このようなルータの障害に対し、ネットワーク間の通信の信頼性を上げるためには、ネットワーク間を2台のルータで接続し、通常は、一方のルータを介して、ネットワーク間の通信をおこない、このルータに障害が発生してメッセージの中継ができなくなった場合には、他方のルータに経路を切り替えるという方法を取る場合がある。

【0006】このように、ルータを2重化しておいて障害があるときに予備のルータを使おうとするときには、ルーティングプロトコルとして、必然的にダイナミックルーティングを採用することになる。

【0007】このダイナミックルーティングの中で、代表的なものとしては、RIP（Routing Information Protocol）がある。RIPは、ネットワークシステムに接続する各計算機とルータが互いに経路情報を交換し、交換した経路情報から最短経路となる経路情報のみ取り出し、保有するという経路制御方法を規定したプロトコルであり、各計算機およびルータは、自分の持つ経路情報より経路を選択してメッセージ通信をおこなう。なお、RIPの規格は、インターネット関連組織の一つである米国NIC（Network Information Center）が発行しているRFC（Request For Comments）1058に規定されている。

【0008】RIPでは、ルータは、一周期（30秒）ごとにネットワークに接続された他のルータに、RIPメッセージと言う経路情報を配布している。そして、各ルータは、最適な経路を選択し、ルーティングをおこなっている。

【0009】ところが、ルータに障害が発生した場合であっても、RIPメッセージを受信してから、6周期（180秒）は、その情報を保持して、正常時と変わりのない動作をおこなう，したがって、予備のルータがあり、それと障害時に切り替えるようにしていても、最低6周期（180秒）は、切り替えがおこなわれず、その間、通信がおこなえなくなる。

5

【0010】

【発明が解決しようとする課題】上記従来技術で述べたＲＩＰは、ＴＣＰ／ＩＰのダイナミックルーティングとしては、現在まで、最も広く用いられてきたルーティングプロトコルである。しかしながら、ルータを２重化していても、ルータに障害が発生してから経路を切り替えるまでには、少なくとも１８０秒間かかり、その間は、通信が途絶するという問題点があった。

【0011】このように、ルータに障害が発生してから経路を切替をするまでの時間を、短縮し、通信が途絶する時間を短縮する方法としては、例えば、以下の方法が考えられている。

【0012】先ず、ネットワーク上にある全てのルータの論理アドレスと、そのルータを経由してたどり着くあて先ネットワークアドレス（ネットワーク全体で、一つのアドレスを対応させたもの）とを対応付けして、予め計算機のメモリに登録しておく。１つのあて先ネットワークに対しては、登録して有るルータの中から特定の１台のルータを使用してメッセージを中継し、同時に、計算機から、このルータあてに、ＲＦＣ７９２で標準化されているＩＣＭＰエコーリクエストメッセージ（ＴＣＰ／ＩＰでは、Ｐｉｎｇというコマンドで定義されている）を周期的に送信する。

【0013】そして、そのルータより、ＩＣＭＰエコーリクエストメッセージに対するＩＣＭＰエコーリプライメッセージが送信されてくるかを一定時間待ち、ＩＣＭＰエコーリプライメッセージを受信しない場合、そのルータに障害が発生したと判断して、予めメモリに登録しておいた他のルータに中継ルータを切り替え、メッセージの通信を継続する。

【0014】この方法によれば、例えば、１５秒おきにＩＣＭＰエコーリクエストメッセージを送信し、送信後、１０秒間ＩＣＭＰエコーリプライメッセージを待つ。そして、１０秒待ってもＩＣＭＰエコーリプライメッセージを受信しない場合には、ＩＣＭＰエコーリクエストメッセージを送ったルータに障害が発生したと判断して、他のルータに中継ルータを切り替える。このようにすると、経路切替時間は、ルータ障害発生から、２５秒で終了することができる。

【0015】しかしながら、この方法は、計算機のメモリ上に実装された通信プログラムをＣＰＵが解釈実行する形態をとるために、計算機のＣＰＵの負荷を増加させるという問題点があった。

【0016】本発明は、上記問題点を解決するためになされたもので、その目的は、ルータが２重化されたネットワークシステムにおいて、現用のルータから予備用のルータに経路を切り替えるときには、その切替時間をＲＩＰ使用時より短縮し、ネットワークの可用性を向上させ、かつ、計算機のＣＰＵの負荷を増加させることのないルータが２重化されたネットワークシステムおよびルータが２重化されたネットワークシステムの障害対策方法を提供することにある。

6

【0017】

【課題を解決するための手段】上記目的を達成するために、本発明のルータが２重化されたネットワークシステムに係る発明の構成は、一つ以上のネットワークをルータを介して接続し、しかも、そのルータが２重化されたネットワークシステムにおいて、前記ネットワークに接続された計算機は、通信制御装置を有し、この計算機は、各々有する通信制御装置によって通信し、また、前記２重化されたルータは、一方を現用ルータ、他の一方を予備用ルータとして、各々同一の論理アドレスと、異なった物理アドレスとが割り当てられ、前記通信制御装置は、前記２重化されたルータの論理アドレスと物理アドレスとを保持する手段を有し、この通信制御装置が、ルータを介して他の計算機と通信するときには、前記現用ルータの物理アドレスを用いて通信し、２重化されたルータに対して、周期的に論理アドレスから物理アドレスを求めるリクエストメッセージを送信し、その送信したリクエストメッセージの返答となるレスポンスメッセージが、ルータから送信されてくるか否かを、２重化された各々のルータに対して監視し、ルータからレスポンスメッセージが送信されてこないときには、そのルータに障害が発生したものとして、もし、前記現用ルータに障害が発生したとされたときには、ルータを介して他の計算機と通信するときに、前記予備用ルータの物理アドレスを用いて通信するように切り替えるようにしたものである。

【0018】より詳しくは、上記ルータが２重化されたネットワークシステムにおいて、前記通信制御装置が、前記２重化されたルータに割り当てられる論理アドレスと物理アドレスとを、計算機より受け取って、それらを２重化されたルータの論理アドレスと物理アドレスとを保持する手段に設定するようにしたものである。

【0019】また別に詳しくは、ルータが２重化されたネットワークシステムにおいて、前記通信制御装置が、前記２重化されたルータに割り当てられる論理アドレスと物理アドレスとを、２重化されたルータ各々に対して送信される前記論理アドレスから物理アドレスを求めるリクエストメッセージの返答となるレスポンスメッセージから得て、それらを２重化されたルータの論理アドレスと物理アドレスとを保持する手段に設定するようにしたものである。

【0020】さらに詳しくは、上記ルータが２重化されたネットワークシステムにおいて、前記現用ルータに障害が発生されたときには、前記予備用ルータを新たな現用ルータとし、現用ルータを取換えて、新たな予備用ルータとして、前記通信制御装置が、２重化されたルータの論理アドレスと物理アドレスとを保持する手段に、前記新たな現用ルータと前記新たな予備用ルータとに割り

当てられる論理アドレスと物理アドレスとを、それぞれ設定するようにしたものである。

【0021】またより具体的に詳しくは、上記ルータが2重化されたネットワークシステムにおいて、前記物理アドレスが、MAC（Media Access Control）アドレスであり、前記論理アドレスが、IP（Internet Protocol）アドレスであり、前記論理アドレスから、物理アドレスを求めるリクエストメッセージが、ARP（Address Resolution Protocol）リクエストメッセージで、その返答となるレスポンスメッセージが、ARPレスポンスメッセージであるようにしたものである。

【0022】上記目的を達成するために、本発明のルータが2重化されたネットワークシステムの障害対策方法に係る発明の構成は、一つ以上のネットワークをルータを介して接続し、しかも、そのルータが2重化されたネットワークシステムの障害対策方法において、前記ネットワークに接続された計算機は、通信制御装置を有し、この計算機は、各々有する通信制御装置によって通信し、また、前記2重化されたルータは、一方を現用ルータ、他の一方を予備用ルータとして、各々同一の論理アドレスと、異なった物理アドレスとが割り当てられ、前記通信制御装置は、前記2重化されたルータの論理アドレスと物理アドレスとを保持する手段を有し、この通信制御装置が、ルータを介して他の計算機と通信するときには、前記現用ルータの物理アドレスを用いて通信し、2重化されたルータに対して、周期的に論理アドレスから物理アドレスを求めるリクエストメッセージを送信し、その送信したリクエストメッセージの返答となるレスポンスメッセージが、ルータから送信されてくるか否かを、2重化された各々のルータに対して監視し、ルータからレスポンスメッセージが送信されてこないときには、そのルータに障害が発生したものとして、もし、前記現用ルータに障害が発生したとされたときには、ルータを介して他の計算機と通信するときに、前記予備用ルータの物理アドレスを用いて通信するように切り替えるようにしたものである。

【0023】より詳しくは、上記ルータが2重化されたネットワークシステムの障害対策方法において、前記通信制御装置が、前記2重化されたルータに割り当てられる論理アドレスと物理アドレスとを、計算機より受け取って、それらを2重化されたルータの論理アドレスと物理アドレスとを保持する手段に設定するようにしたものである。

【0024】また別に詳しくは、ルータが2重化されたネットワークシステムの障害対策方法において、前記通信制御装置が、前記2重化されたルータに割り当てられる論理アドレスと物理アドレスとを、2重化されたルータ各々に対して送信される前記論理アドレスから物理アドレスを求めるリクエストメッセージの返答となるレスポンスメッセージから得て、それらを2重化されたルータの論理アドレスと物理アドレスとを保持する手段に設定するようにしたものである。

【0025】さらに詳しくは、ルータが2重化されたネットワークシステムの障害対策方法において、前記現用ルータに障害が発生されたときには、前記予備用ルータを新たな現用ルータとし、現用ルータを取換えて、新たな予備用ルータとして、前記通信制御装置が、2重化されたルータの論理アドレスと物理アドレスとを保持する手段に、前記新たな現用ルータと前記新たな予備用ルータとに割り当てられる論理アドレスと物理アドレスとを、それぞれ設定するようにしたものである。

【0026】より具体的に詳しくは、ルータが2重化されたネットワークシステムの障害対策方法において、前記物理アドレスが、MAC（Media Access Control）アドレスであり、前記論理アドレスが、IP（Internet Protocol）アドレスであり、前記論理アドレスから、物理アドレスを求めるリクエストメッセージが、ARP（Address Resolution Protocol）リクエストメッセージで、その返答となるレスポンスメッセージが、ARPレスポンスメッセージであるようにしたものである。

【0027】

【発明の実施の形態】以下、本発明に係る各実施形態を、図1ないし図19を用いて説明する。

【0028】〔TCP／IPに関する一般的事項〕先ず、本発明の実施形態の理解を容易にするために、図2ないし図4を用いてTCP／IPの一般的事項について簡単に説明する。最初に、図2を用いてIPアドレスの概念から説明する。図2は、IPアドレスの各クラスの形態を模式的に示した図である。

【0029】IPアドレスとは、TCP／IPの通信規約において、通信に参加する計算機（TCP／IPの用語では、「ホスト」という）などのエンテティ（「ノード」ともいう）に割り当てられるネットワーク上で一意的なアドレスである。

【0030】IPアドレスは、32ビットの整数で表現され、図2（a）に示されているように、ネットワークIDとホストIDで構成されている。ネットワークIDは、ネットワークを識別するIDであり、ホストIDは、そのネットワーク上でホストを識別するIDである。

【0031】このIPアドレスには、利用するネットワークの形態によってクラスが設けられていて、図1にはその内でAクラスからCクラスまでが図示されている。IPアドレスがどのクラスに属するかは、ネットワークIDの先頭ビットのパターンで識別するようになっている。

【0032】図からわかるように、Aクラスほどホストビット数が大きくなっており、従って、大規模なネットワークで用いることになる。反対に、Cクラスは、ホストIDは、8ビットしか持っていないため、小

規模なネットワーク向きであるといえる，

【００３３】上記の様に、ＩＰアドレスは、３２ビットのビット列であったが、これを表記するために、８ビット単位で区切ってそれを１０進数で表わす、いわゆるオクテット表示が用いられるのが、一般的になっている。例えば、２進数のビット列で、（１０００００１０　００００００１　００００１００　００００１０００）と表わされるＩＰアドレスは、「１３０．１．４．８」と表記される。本明細書でも、以下このオクテット表示を用いることにする。

【００３４】また、一つのネットワークをＩＰアドレスで識別したいときには、これをネットワークアドレスて呼び、ＩＰアドレスの内のホストＩＤを０として表記することにする。例えば、上記の例の「１３０．１．４．８」は、Ｂクラスに属するので、下位１６ビットがホストＩＤとなり、ネットワークアドレスは、「１３０．１．０．０」となる，

【００３５】次に、ＭＡＣアドレスについて説明する。

【００３６】上記のＩＰアドレスは、各ノードに割り振られるアドレスであったが、このＩＰアドレスよりも、より低位な立場から、割り振られる４８ビットのアドレスが、ＭＡＣ（Media Access Control）アドレスである。したがって、比較して、ＩＰアドレスは、論理的アドレスであり、ＭＡＣアドレスは、物理的アドレスであるということができる。

【００３７】さて、通信プロトコルを説明するための著名なモデルとして、ＯＳＩ（Open Systems Interconnection）参照モデルがある。ここでは、図３を用いて、このＯＳＩ参照モデルによるＴＣＰ／ＩＰでの通信規約と上記のＩＰアドレスとＭＡＣアドレスの関係について概説することにしよう，図３は、ＯＳＩ参照モデルとＴＣＰ／ＩＰの通信プロトコルの関係を示す模式図である。

【００３８】ＯＳＩ参照モデルは、図３（ａ）に示される様に通信機能を階層的にモデルとして表わしたものであり、下位になるほどより物理的な機能を担う層であり、上位は、より論理的な機能を担う層である，このモデルの各層は、特定のサービスを上位層に提供し、特定のサービスを下位層より受け取る。

【００３９】このＯＳＩ参照モデルを、ＴＣＰ／ＩＰの通信規約にあてはめると、図３（ｂ）に示されるようになる，ＯＳＩ参照モデルで、第５層から第７層に該当するのが、上位層に属するＴｅｌｎｅｔ（仮想端末機能）、ＦＴＰ（ファイル転送）などの通信サービスである。

【００４０】その下が、第４層のトランスポート層のプロトコルで、ＴＣＰ（TransmitionControl Protocol）とＵＤＰ（User Datagram Protocol）という通信プロトコルである，また、その下は、第３層のネットワーク層のプロトコルは、ＩＰプロトコルである，（この層をＴＣＰ／ＩＰの用語で、インターネット層ということがある。）

最下層は、電気的な規格や物理的な通信路の確立に関するものであり、代表的な規格としては、イーサネット（Erthenet）がある，（この層をＴＣＰ／ＩＰの用語で、ネットワーク・インターフェース層ということがある。）本明細書の説明でも、イーサネットで通信をおこなうものとして説明する，

【００４１】さて、実際に通信が行われる場合の仕組みについて説明すると、図３（ｃ）に示されるように、送信のときに、下位層にデータを渡して、下位層では、その層のヘッダ情報を付け、逆に、受信のときには、その層のヘッダを解析して、上位層に渡すようになっている，

【００４２】具体的にいうと、最下層では、通信の対象は、イーサネットフレームを受け取る。先頭には、イーサネットヘッダがあり、あて先のＭＡＣアドレスと送信元のＭＡＣアドレスとそのフレームのタイプを示すフレームタイプが含まれている。その後は、この層からみたときのイーサネットデータとなる，一つ上の層のＩＰプロトコルでは、下の層のイーサネットデータを、この層では、ＩＰデータグラムといい、ＩＰヘッダとＩＰデータとからなる。そして、ＩＰヘッダには、あて先のＩＰアドレスと送信元のＩＰアドレスとプロトコルのタイプを示すプロトコルタイプとが含まれている。

【００４３】同様に、その上の層のＴＣＰプロトコルでは、ＩＰデータは、ＴＣＰヘッダとＴＣＰデータとからなる，

【００４４】この様に、各層ではその層のヘッダの処理をおこなうようように、仕様が定められていて、通信の一貫性と各層での処理のモジュール化が図られている。

【００４５】次に、図４を用いてＡＲＰ（Address Resolution Protocol）プロトコルについて説明しよう。図４は、ＡＲＰの仕組みを説明する模式図である。

【００４６】既に述べたように、ＴＣＰ／ＩＰの下位のネットワーク・インターフェース層では、通信のノードのアドレスをＭＡＣアドレスとして、その上位にあたるインターネット層では、ＩＰアドレスとして認識する。そして、ＩＰアドレスによって相手を指定して通信をおこなう際にも、イーサネットフレームを組み立てるので、ＭＡＣアドレスとＩＰアドレスの両者が必要である，ところが、通常、通信に参加するホストは、相手のＩＰアドレスを認識していても、ＭＡＣアドレスを認識していない。そのために、ＩＰアドレスからＭＡＣアドレスを知るためのプロトコルが、ＡＲＰである。このＡＲＰに使われるメッセージには、ＡＲＰリクエストメッセージとＡＲＰレスポンスメッセージの二種類が有る。

【００４７】ここで、図４に示されるネットワーク構成のシステムがあったとする。

【００４８】（１）ノードＡがノードＣと通信をおこないたいとする，ＣのＩＰアドレスは、１６０．１６０．